Remarks/Arguments

The examiner claims that:

With regard to claim 26, e-Security discloses:

collecting real-time operation information on one or more first elements of a network (e-Security: Page 13. As shown in the figure, e-Security agents are utilized to collect information from disparate sources and correlate the information in a database.).

but admits that:

e-Security does not disclose expressly:

selecting a policy to be implemented by at least one second network element different from the first network element, responsive to the collected real time information from the one or more first network elements, the at least one second element including an endpoint of the network and hosting an agent, and enforcing the selected policy on the agent hosted by the at least one second network element.

a system where a proxy (agent) is deployed onto a network element and is used to perform the operations defined by a configuration plan to change the settings of the network element (Mattila: Figure 2 and paragraph [0005]).

is substantially different from:

selecting a policy to be implemented by at least one second network element different from the first network element, responsive to the collected real time information from the one or more first network elements, the at least one second element including an endpoint of the network and hosting an agent, and enforcing the selected policy on the agent hosted by the at least one second network element.

because unlike the e-Security and Mattila systems, the proposed system performs real-time selection of an enforceable policy in response to real-time operational input data collected from one set of network elements and implementation of this policy on another set of network elements.

Thus, it is respectively submitted that claim 26 is not obvious in light of the combination of

e-Security and Mattila and therefore allowance thereof is respectfully requested.

The examiner claims that:

With regard to claim 27, e-Security as modified by Mattila teaches that collecting real-time operation information comprises collecting information on operation problems (e-Security: Page 8. e-Security can view the status of different devices along with logged information in the devices. Thus, the information may be related to operational problems depending on the status of the devices.).

But the e-Security specification directly refers to the collection of unprocessed security-oriented information that indicates status and/or alerts:

Holistic View
e-Sentinel receives all of the relevant alert information from various sources distributed throughout the enterprise, prioritizes them with the appropriate severity level, stores the normalized data and performs correlation – all in real time from one central control center. e-Sentinel is robust enough to manage all existing security point products on the market as well as flexible in its architecture to encompass emerging technologies. e-Sentinel directly addresses the need of today's Security staff to centrally monitor all of their distributed security environment from a central control center. This includes the ability to view the status of enterprise security and information assets such as:

- Information security devices (e.g. firewalls, IDS)
- Network devices (for security events)
- Applications and services (e.g. OS, databases, e-mail)
- File servers & Enterprise Resource Planning (ERP) Systems
- Other security sources (e.g. badge readers, process control devices)
- Information assets grouped by business unit, business process, or enterprise initiative

This is substantially different from the proposed system which unlike the e-Security and Mattila systems, performs real-time selection of an enforceable policy in response to operational problems collected from one set of network elements and implementation of this policy on another set of network elements.

Thus, it is respectively submitted that claim 27 is not obvious in light of the combination of

e-Security and Mattila and therefore allowance thereof is respectfully requested.

The examiner claims that:

With regard to claim 28, e-Security as modified by Mattila teaches that collecting real-time operation information comprises collecting information on software applications installed or running on network elements (e-Security: Page 15. e-Security collects data from operating systems, which includes software applications running on network elements.).

But the e-Security document only mentions:

Operating Systems:

- Windows NT (Microsoft)
- Windows 2000 (Microsoft)
- Solaris (Sun)
- SunOS (Sun)
- HP-UX (Hewlett-Packard)
- IRIX (Silicon Graphics)
- AIX (IBM)
- ~~Linux (Various)~~
- Digtal UNIX/Tru64 UNIX (Compaq)

This does not include disclosure of the monitoring of software applications running under these operating systems. Claim 28 deals with the collection of information about applications that are not operating or operating slowly which is substantially different from alert and status information collection from a host operating system.

Thus, it is respectively submitted that claim 28 is not obvious in light of the combination of

e-Security and Mattila and therefore allowance thereof is respectfully requested.

The examiner claims that:

With regard to claim 29, e-Security as modified by Mattila teaches the invention as substantially claimed except that collecting real-time operation information comprises collecting information on system or application crashes.

but only refers to system crashes as known in the art:

However, Official Notice is taken that it was well known in the art to collect information on system crashes.

Thus, it would have been obvious to collect information on system crashes in the disclosure of e-Security as modified by Mattila.

The suggestion/motivation for doing so would have been that e-Security is concerned with collecting information on security events. A crashed system may be symptomatic of certain types of attacks that the network administrator should be made aware of.

The detection of application crashes is substantially different from system crashes because it requires direct interaction by the agent with the operating system software. This is not referred to or implied by e-Security.

As it pertains to system crashes, claim 29 is substantially different from e-Security modified by Mattila, as it performs real-time selection of an enforceable policy in response to system crashes collected from one set of network elements and implementation of this policy on another set of network elements.

Thus, it is respectively submitted that claim 29 is not obvious in light of the combination of

e-Security and Mattila and therefore allowance thereof is respectfully requested.

The examiner claims that:

> With regard to claim 30, e-Security as modified by Mattila discloses that collecting information comprises collecting information on software applications installed or running on the network elements (e-Security: Page 15. Information may be collected on at least anti-virus software and operating systems.).

but specifically mentions the operating system status and anti-virus software. This is substantially different from generic collection of any software installed and used on the host because it requires direct interaction by the agent with the operating system software. This is not referred to or implied by e-Security.

Thus, it is respectively submitted that claim 30 is not obvious in light of the combination of e-Security and Mattila and therefore allowance thereof is respectfully requested.

The examiner claims that:

> With regard to claim 31, e-Security as modified by Mattila teaches that collecting real-time operation information comprises collecting information on the communications between elements of the network (e-Security: Page 15. Included in the devices that are monitored are intrusion detection, firewalls, and authentication, all of which include information on some communication between elements on the network.).

But the reference to intrusion detection, firewalls and authentication network nodes by the e-Security system is in regards to event information (e.g.: SNMP trap or a log file) within such node rather than complete communication awareness. As explained by e-Security in page 14:

Key Benefits of Agents:

- Ability to collect event information from any device that generates either SNMP trap or a log file
- Normalization of event information reported in disparate languages from any device in the security environment
- Event filtering and reduction of false positives
- Customizable and easy to add when needed
- Encompasses best practices and other industry standards
- Minimal use of processing power and network bandwidth

This is substantially different from monitoring of each communication path of the network node because requiring the IDS or Firewall system to output a log entry for each communication between network elements would greatly disrupt the network performance.

Thus, it is respectively submitted that claim 31 is not obvious in light of the combination of e-Security and Mattila and therefore allowance thereof is respectfully requested.

The examiner claims that:

With regard to claim 32, e-Security as modified by Mattila teaches the invention as substantially claimed except that selecting the policy to be implemented comprises selecting a policy relating to a software to be installed on the second network element.

However, official notice is taken that automatic updates of software were well known in the art.

Thus, it would have been obvious to have the configuration plan of -Security as modified by Mattila relating to software to be installed.

And further specifies:

The suggestion/motivation for doing so would have been that often times merely changing the settings of a network element is not enough to correct a problem in a network, or to bring an element in line with the desires of a network administrator. Thus, having the configuration plan include information on where to fetch software and have instructions to install the software would allow e-Security as modified by Mattila to enjoy a higher level of automation.

unlike a combination an automatic update system which strives to have the most up-to-date version of a specific software with the e-Security and Mattila systems, the proposed system performs real-time selection of an enforceable installation policy in response to real-time operational input data collected from one set of network elements and implementation of this installation policy on another set of network elements.

Thus, it is respectively submitted that claim 32 is not obvious in light of the combination of e-Security and Mattila and therefore allowance thereof is respectfully requested.

The examiner claims that:

With regard to claim 33, e-Security as modified by Mattila teaches the invention as substantially claimed except that selecting the policy to be implemented comprises selecting a policy relating to a software to be uninstalled from the second network element.

However, official notice is taken that automatic uninstalling software was well known in the art.

Thus, it would have been obvious to have the configuration plan of -Security as modified by Mattila relating to software to be uninstalled.

And further specifies:

The suggestion/motivation for doing so would have been that often times merely changing the settings of a network element is not enough to correct a problem in a network, or to bring an element in line with the desires of a network administrator. Thus, having the configuration plan include information on where to fetch software and have instructions to uninstall the software would allow e-Security as modified by Mattila to enjoy a higher level of automation.

unlike a combination an automatic un-installation system which is geared towards licensing of software with the e-Security and Mattila systems, the proposed system performs real-time selection of an enforceable uninstallation policy in response to real-time operational input data collected from one set of network elements and implementation of this installation policy on another set of network elements.

Thus, it is respectively submitted that claim 33 is not obvious in light of the combination of e-Security and Mattila and therefore allowance thereof is respectfully requested.

The examiner claims that:

With regard to claim 34, e-Security as modified by Mattila teaches the invention as substantially claimed except that selecting the policy to be implemented comprises selecting a policy relating to preventing the installation of a software on the second network element.

However, it was well known in the art to prevent installation of software on network elements.

Accordingly, it would have been obvious to have the policy relate to preventing the installation of a software on the second network element.

And further specifies:

The suggestion/motivation for doing so would have been that there would have been many reasons to prevent the installation of software. First, the software may have a known security vulnerability, thus making it undesirable to deploy the software on a large scale in a network. Further, virus and spyware scanners are concerned with preventing software to be installed, meaning that having the policy involve updating virus/spyware scanners would mean that the policy relates to preventing the installation of a software, where the software is a virus or spyware.

Unlike a combination of a static list of unauthorized software or an anti-virus which prevents installation of applications matching a viral signature with the e-Security and Mattila systems, the proposed system performs real-time selection of an enforceable installation prevention policy in response to real-time operational input data collected from one set of network elements and implementation of this installation policy on another set of network elements. This would be comparable to an anti virus system that learns new signatures depending on the behavior of viruses on other parts of the network.

Thus, it is respectively submitted that claim 34 is not obvious in light of the combination of e-Security and Mattila and therefore allowance thereof is respectfully requested.

The examiner claims that:

With regard to claim 35, e-Security as modified by Mattila teaches the invention as substantially claimed except that selecting the policy to be implemented comprises selecting responsive to a determination that a group of network elements having a common problem have installed thereon a specific software application or combination of software applications.

However, a person of ordinary skill in the art would have known how to perform this functionality.

Thus, it would have been obvious to have selecting the policy to be implemented comprises selecting responsive to a determination that a group of network elements having a common problem have installed thereon a specific software application or combination of software applications.

But points out that e-Security are providing event correlation to outline the connection between different events:

The suggestion/motivation for doing so would have been that e-Security is concerned with correlating events to allow connections between different events to be seen. Thus, if a combination of software applications is causing a problem, the information that was correlated could show this problem, and thus assist in determining the solution to the problem.

Performing event correlation to find the connection between different events is substantially different from selecting a policy responsive to a common problem caused by an installation of a software application or a combination of software applications. An event correlation mechanism finds common outcomes of a problem rather than the cause and the policy to implement in response to it.

Thus, it is respectively submitted that claim 35 is not obvious in light of the combination of e-Security and Mattila and therefore allowance thereof is respectfully requested.

The examiner claims that:

With regard to claim 36, e-Security as modified by Mattila teaches selecting a policy relating to allocation of network resources (e-Security: Page 15. Deploying any policy to firewalls or authentication devices relates to allocation of network resources, as these device are directly involved in the allocation of network resources. It is noted that the instant claim provides no detail on what constitutes "relating," thus meaning that a policy having any relation to allocation of any network resource meets the claim language.).

but the e-Security Page 15 outlines that:

Integrated Products
The following is a representative list of the products that e-Security has integrated with during the course implementing the Open e-Security Platform at our customer sites. This list grows daily as e-Security and our customers design new Agents to monitor other devices for security event information:

Dynamic network resource allocation is significantly different from combining the collection of security events and a proxy configurator because unlike the e-Security and Mattila systems, the proposed system performs the real-time selection of an enforceable network resource allocation policy in response to real-time operational input data.

Thus, it is respectively submitted that claim 36 is not obvious in light of the combination of e-Security and Mattila and therefore allowance thereof is respectfully requested.

The examiner claims that:

With regard to claim 37, e-Security as modified by Mattila teaches the invention as substantially claimed except that the policy is selected within less than 60 minutes from the collection of the information.

However, having the policy selected (not necessarily implemented) within 60 minutes from the collection of the information would have been well known to a person of ordinary skill in the art.

Thus, it would have been obvious to have the policy selected within 60 minutes from the collection of the information.

The suggestion/motivation for doing so would have been that having a problem resolved as quickly as possible allows the network to become error free as quickly as possible, thus resulting in less potential loss.

because unlike the e-Security and Mattila systems, the proposed system performs real-time selection of an enforceable policy in response to real-time operational input data collected from one set of network elements and implementation of this policy on another set of network elements, having the policy selected rapidly, in less than 60 minutes, is novel.

Thus, it is respectively submitted that claim 37 is not obvious in light of the combination of e-Security and Mattila and therefore allowance thereof is respectfully requested.

The examiner claims that:

With regard to claim 38, e-Security as modified by Mattila teaches that collecting the operation information is performed repeatedly (e-Security: page 10. e-Security provides real-time awareness, meaning that the information is collected in real-time).

But unlike the e-Security and Mattila systems, in addition to the collection of operational information, the proposed system performs real-time selection of an enforceable policy in response to real-time operational input data collected from one set of network elements and implementation of this policy on another set of network elements.

Thus, it is respectively submitted that claim 38 is not obvious in light of the combination of e-Security and Mattila and therefore allowance thereof is respectfully requested.

The examiner claims that:

With regard to claim 39, e-Security as modified by Mattila teaches that the method is adapted to select the policy to be implemented by the at least one second network element responsive to operation information collected from at least 2 first network elements (e-Security: Page 15. Alerts are generated based on collected

Specifically referring to alerts:

network elements (e-Security: Page 15. Alerts are generated based on collected information from many network elements.).

Unlike the e-Security and Mattila systems where events would be monitored and alerts generated, the proposed system performs real-time selection of an enforceable policy in response to real-time operational input data collected from one set of network elements and implementation of this policy on another set of network elements.

Thus, it is respectively submitted that claim 39 is not obvious in light of the combination of e-Security and Mattila and therefore allowance thereof is respectfully requested.

The examiner claims that:

With regard to claim 40, the disclosed invention is substantially similar that of claim 26, and is rejected for substantially similar reasons.

As argued for claim 26, because unlike the e-Security and Mattila systems, the proposed system performs real-time selection of an enforceable policy in response to real-time operational input data collected from one set of network elements and implementation of this policy on another set of network elements.

Thus, it is respectively submitted that claim 40 is not obvious in light of the combination of e-Security and Mattila and therefore allowance thereof is respectfully requested.

The examiner claims that:

With regard to claim 41, e-Security as modified by Mattila teaches that the processor is adapted to find, for a group of network elements having a problem, a combination of attribute values that correlate with the problem to at least a predetermined degree (e-Security: Page 10, "Correlation." e-Security correlates events

but refers specifically to event attributes:

predetermined degree (e-Security: Page 10, "Correlation." e-Security correlates events that may be related based on attributes of the event.).

Clarifying that the correlation mechanism e-Security applies is specific to the attributes of the collected events rather than the attributes of the network elements. Performing correlation on the event attributes to generate an alarm is a substantially different

approach to finding attributes that have a causal relationship with a group of nodes suffering from a problem.

Thus, it is respectively submitted that claim 41 is not obvious in light of the combination of e-Security and Mattila and therefore allowance thereof is respectfully requested.

The examiner claims that:

With regard to claim 42, e-Security as modified by Mattila teaches the invention as substantially claimed except that the processor is adapted to find, for a group of network elements having a problem, a combination of attributes values that appears only on the network elements having the problem.

Explaining that the purpose of the event correlation is finding all related events:

The suggestion/motivation for doing so would have been that e-Security is intended to correlate events to find all the information that is relevant to a single event. Thus, finding a common attribute that is only on affected systems appears to be the intention of the correlation, which would allow connections to be found between the different elements.

The correlation mechanism e-Security applies is specific to the attributes of the collected events rather than the attributes of the network elements. Performing correlation on the event attributes in order to generate an alarm is a substantially different approach to finding attributes that have a causal relationship with a group of all nodes suffering from a specific problem.

Thus, it is respectively submitted that claim 42 is not obvious in light of the combination of e-Security and Mattila and therefore allowance thereof is respectfully requested.

The examiner claims that:

> With regard to claim 43, e-Security as modified by Mattila teaches that the processor is adapted to collect for at least one network element, a plurality of snapshot records of the network element at different times (e-Security: Page 13. The agents collect information in a continuous fashion from different event sources.).

but the reference for e-Security as modified by Mattila does not teach a system that collects a plurality of snapshots of collected network element attribute information, but rather correlates and normalizes events.

Thus, it is respectively submitted that claim 43 is not obvious in light of the combination of e-Security and Mattila and therefore allowance thereof is respectfully requested.

The examiner claims that:

> With regard to claim 44, e-Security as modified by Mattila teaches that the processor is adapted to verify that each network element belongs to the network before collecting information from the network element (e-Security: page 13. There is no requirement as to what is meant by "belongs to the network." Being connected to a network constitutes "belong to the network." e-Security can only collect information from nodes that "belongs to the network." Therefore, if information is received, the node "belongs to the network.").

Thus, it is respectively submitted that claim 44 is not obvious in light of the combination of e-Security and Mattila and therefore allowance thereof is respectfully requested.

The examiner claims that:

With regard to claim 45, e-Security as modified by Mattila teaches the invention as substantially claimed except that the processor is adapted to find groups using a k-clustering or hierarchy clustering method.

However, a person of ordinary skill in the art would have known how to have the processor of e-Security as modified by Mattila find groups using a k-clustering or hierarchy clustering method.

Thus, it would have been obvious to have processor of e-Security as modified by Mattila find groups using a k-clustering or hierarchy clustering method.

Specifically pointing out clustering as used for network segmentation:

The suggestion/motivation for doing so would have been that both k-clustering and hierarchy clustering methods divide the network into smaller portions in order to facilitate different processes within the network. For example, k-clustering divides the network into non-overlapping sub networks, which then allows the monitoring and policy functions of e-Security as modified by Mattila to be performed with respect to the sub networks as far as collection and deployment, but correlated in a centralized fashion to allow the necessary correlation activities to be performed.

However, the use of finding groups is for policy transmission which is substantially different from the use of clustering to perform network subdivisions for purposes of event collection because it applies to enforcing different policies for different groups within the network. The combination of e-Security and Mattila do not perform such subdivisions.

Thus, it is respectively submitted that claim 45 is not obvious in light of the combination of e-Security and Mattila and therefore allowance thereof is respectfully requested.

CONCLUSION

In light of the foregoing, Applicant respectfully submits that all rejections have been responded to and that the pending claims are in condition for allowance.

A Petition for Extension of Time accompanies this Amendment along with authorization to charge the appropriate fees to Deposit Account No. 06-0923. It is believed that no additional fees are necessitated by the present Response. However, in the event that any additional fees are due, the Commissioner is hereby authorized to charge any such fees to Deposit Account No. 06-0923. The Commissioner is likewise authorized to credit any overpayment to Deposit Account No. 06-0923.

If the Examiner believes that a telephone conversation with Applicant's attorney would expedite allowance of this application, the Examiner is cordially invited to telephone the undersigned attorney at the number provided below.

Dated: February 19, 2009

Respectfully submitted,

Electronic signature: /Richard I. Samuel/
Richard I. Samuel
Registration No.: 24,435
GOODWIN PROCTER LLP
The New York Times Building
620 Eighth Avenue
New York, New York 10018
(212) 813-8800
Attorney for Applicant